Asian Journal of Information Technology 6 (4): 441-446, 2007

Wireless Lan Security: An In-Depth Study of the Threats and Vulnerabilities

Rony Hasinur Rahman, Nusrat Nowsheen, Mahbubul Azam Khan and Asif Hossain Khan
Department of Computer Science and Engineering, University of Dhaka, Dhaka-1000, Bangladesh

Abstract: As the wireless communications is coming to the offices and the homes, there are some new security issues to take care. Today we have continuously growing markets for the wireless LANs, but there is a big black hole in the security of this kind of networks. This study explores and analyzes the threats and vulnerabilities of wireless LANs. The research is intended to help business owners and network administrators understand the key elements that a secure wireless network requires so they can avoid the expense and risk associated with an inadequate deployment. The study also provides background information, suggestions and guidelines for assessing the various types of wireless security solutions available using today's technology.

Key words: Access Point (AP), Rogue AP, Man-In-The-Middle (MITM), eavesdropping, SSID (Service Set Identifier), RF (Radio Frequency), wardriving

INTRODUCTION

Organizations of all sizes are installing and operating wireless networks, known as Wireless Local Area Networks (WLANs) or Wi-Fi networks. The benefits that are propelling the widespread adoption of wireless technology are low cost, ease of installation and flexibility. While the benefits of WLANs are substantial, wireless technology introduces security holes that network administrators must take into account if they are to adequately protect their organizations from hackers, cyber terrorists and unauthorized intruders. Wireless networks are notoriously easy to compromise when improperly installed and operated. Once compromised, a WLAN gives intruders an open conduit to the entire network and places all proprietary and mission-critical information in jeopardy. Wireless security is not impossible to achieve. It also does not impose an additional management burden on IT staff. In fact, when a comprehensive, layered-security approach is implemented, a WLAN can be more secure and easier to use and manage than a typical wired network. Next we skim through the advantages and drawbacks of wireless technology (Mitchell, 2004).

WIRELESS ADVANTAGES

The operational characteristics described in the previous paragraphs give rise to a number of advantages that are driving wireless technologys growing popularity. The advantages are briefly described below.

Increased productivity and flexibility: Wireless users can move throughout the coverage area-from offices to conference rooms, from the lunch-room to the shop floor-without disconnecting from the network. A study conducted by NOP (Network Operator) World found that wireless users stay connected to the network an average of 1.75 h longer per day, which translates roughly to a 20% increase in productivity.

Ease of installation: A LAN could be operational in a matter of hours, whereas a wired network might take days or weeks to install.

Cost: WLANs can be installed more economically than wired LANs. On average, adding users to a wired LAN costs approximately $130 per connection, so extending coverage to new office space for 50 users would cost about $6500. The same space could be covered by a single WAP (~ $150) and 50 NICs (~ $60 per card) for a total cost of approximately $3150 (Mitchell, 2004).

WIRELESS RISKS AND VULNERABILITIES

The same characteristics that make WLANs attractive also create a number of serious and potentially catastrophic vulnerabilities. Some of these risks are mentioned below.

The nature of the wireless medium: Traditional wired networks use cables to transfer information, which are protected by the buildings that enclose them. To access a wired network, a hacker must bypass the physical

Corresponding Author: Rony Hasinur Rahman, Department of Computer Science and Engineering, University of Dhaka, Dhaka-1000, Bangladesh

security of the building or breach the firewall. On the other hand, wireless networks use the uncontrolled medium. Wireless LAN signals can travel through the walls, ceilings and windows of buildings up to thousands of feet outside of the building walls. Additionally, since the WLAN medium is airwaves, it is a shared medium that allows any one in proximity to sniff the traffic. The risks of using a shared medium is increasing with the advent of readily-available hackers tools. A variety of specialized tools and tool kits enable hackers to sniff data and applications and to break both the encryption and authentication of wireless data.

Insecure wireless LAN devices: Insecure wireless LAN devices, such as access points and user stations, can seriously compromise both the wireless network and the wired network, making them popular targets for hackers.

Insecure access points: Access points can be insecure, due to improper configurations and design flaws. Access points ship with default configurations that are insecure. They are pre-configured with a default password; they broadcast Service Set Identifiers (SSIDs) and they often require no encryption or authentication. If deployed with default settings, they become gateways that hackers use to access both the wireless and the wired network.

Insecure user stations: Insecure wireless user stations such as laptops or bar code scanners pose even a greater risk to the security of the enterprise network than insecure access points. The default configuration of these devices offer little security and can be easily misconfigured. Intruders can use any insecure wireless station as a launch pad to breach the network. Access points can also be reset to default settings by a power surge, system failure, or a reset button (Wireless LAN Security, 2004).

This study introduces wireless security threats and suggests steps that can be taken to operate a WLAN in a secure manner. This study intends to help IT professionals considering wireless additions to their LANs as well as those already operating WLANs in their network environment (Mitchell, 2004).

DIFFERENT WIRELESS THREATS

The vulnerabilities of wireless LAN can be exploited easily by various means. Different types of attacks that can be used to break into a wireless LAN are given in Table 1.

Table 1: Different types of attacks

Attacks	Description
Probing/Network discovery	Allows hackers to find and try to enter the network
Denial of Service (DoS)	Denies legitimate users from accessing the network
Surveillance	Allowing unauthorized viewing of data
Impersonation	Allows unauthorized users to spoof authorized users and devices
Rogue APs and Ad Hoc Networks	Unauthorized Aps and clients provide unrestricted access to network

Probing/network discovery: Network discovery is a normal part of the 802.11 protocol that lets clients learn about available services. Without it, legitimate users can't access the network. However, network discovery mechanisms also allow malicious users in search of free Internet access, as well as potential hackers, to find and look for entry into the corporate network. Network discovery in 802.11 works in one of two ways: Passive discovery mode and active discovery mode. In passive discovery mode, a station simply listens for beacon transmissions coming from Access Points (APs). These beacon frames normally contain the SSID of the network as well as clock synchronization data and other parameters regarding capabilities of the AP. Once a passive station detects these beacons, it displays the SSID to the user. In active discovery mode stations actively send out messages called probe requests to APs in the area. These probe requests can be either broadcast, meaning they are searching for any network or specifically looking for a pre-configured SSID. APs respond to probe requests with probe response messages (Joris *et al*., 2002; Secure Wireless, 2004).

Denical of Service (DoS): The goal of any Denial of Service (DoS) attack is to ultimately prevent legitimate users from accessing the wireless LAN-either for an extended period of time or just for a moment in order to carry out a specific attack. Wireless DoS attacks are classified into two major categories: RF attacks and 802.11 attacks. RF attacks are typically referred to as jamming. They involve an attacker using some type of radio transmitter to generate noise in the 2.4GHz or 5GHz spectrum with the end goal of disrupting all radio communication in that frequency band. 802.11 equipment is designed to operate above a certain signal-to-noise ratio and in the presence of RF jamming will typically not be able to communicate at all. There is little that can be done to stop RF jamming. What's needed is the ability to have APs detect signal-to-noise ratio and notify the network manager when it drops below a certain threshold. If the jamming is only on a specific 802.11 channel, APs also need the ability to search for a better channel. Fortunately, jamming is rare-owing both to the cost of equipment and the fact that it is illegal in most countries. The second and more common type of DoS attack works within the 802.11 protocol framework. These types of attacks require only a laptop or PDA with a wireless

NIC-equipment that is inexpensive and readily available. These attacks range from floods of 802.11 associate frames that attempt to consume all available client slots in the AP to 802.1×EAP (Extensible Authentication Protocol) handshake floods that try to overwhelm an authentication server to the ubiquitous deauthenticate (i.e., deauth) flood that causes clients to drop their association with an AP. Deauth attacks are the most effective of 802.11 DoS attacks. They exploit a weakness in the 802.11 protocol that forces stations and APs to use the source MAC address as the identifier of another 802.11 device. Frames are not authenticated-meaning that anyone can change the MAC address of their NIC card and send frames that appear to come from another device. Attackers exploit this weakness to send deauthenticate frames to stations that appear to come from the AP-stations respond according to the protocol requirements and drop their association to the AP. If this process is repeated enough times, stations will assume the wireless LAN is no longer available and will begin scanning for a new AP (Claire, 2003).

Surveillance: Armed with a wireless network adaptor that supports promiscuous mode, the eavesdropper can capture network traffic for analysis using easily available tools, such as Network Monitor in Microsoft products, or TCPdump in Linux-based products or AirSnort. Eavesdropping on a wireless network may not be malicious in nature. In fact, many in the wardriving community claim their wardriving activities are benign or educational in nature. It is worth noting that wardriving, looking for and detecting wireless traffic, is probably not illegal, even though propagandistic claims to the contrary are often made. Wireless communication takes place on unlicensed public frequencies-any one can use these frequencies. This makes protecting a wireless network from eavesdropping more difficult (Robert, 2004a-c).

IMPERSONATION

Type 1: The first type of impersonation is MAC Spoofing (Identity Theft). The theft of an authorized user's identity is a serious threat to wireless networks. Even though SSIDs and Media Access Control (MAC) addresses act as Personal Identification Numbers (PINs) for verifying the identity of authorized clients, existing encryption standards are not foolproof. Knowledgeable hackers can pick off authorized SSIDs and MAC addresses and steal bandwidth, corrupt or download files and wreak havoc on the entire network. Some enterprises secure their wireless LAN by using an authorized list of station MAC addresses for authentication. While this method provides some security for smaller deployments, MAC addresses were never intended for this use. Even if encryption or VPN is used, MAC addresses are always in the air. With software tools such as Kismet or Ethereal®, a hacker can easily capture the MAC address of a valid user. To perform identity theft, a hacker can change his MAC address to the victim's MAC address using a spoofing utility such as SMAC (Spoof MAC) or, manually change the Windows registry entry. Once this has been done, the hacker can connect to the wireless LAN, bypassing any MAC address filtering (Chang, 2002).

Type 2: One of the more sophisticated attacks, the Man-in-the-Middle attack, breaks VPN connections between authorized stations and access points by inserting a malicious station between the victim's station and the access point. The hacker becomes the man in the middle. These attacks are very similar to wired side Man-in-the-Middle attacks and tools to exploit these attacks on the wired-side can be easily used on the wireless network. Getting into the middle of a communication session is a problem on the wired side. This process is much easier with wireless networks. Using SoftAP software, a hacker can easily convert a wireless device into a soft access point and position that access point in the middle of the communication session. The more sophisticated Man-in-the-Middle attack preys upon challenge and handshake protocols to perform a de-authentication attack. The de-authentication attack knocks a user from an access point, causing the user to search for a new access point with which to connect. With the hacker's SoftAP access point running, the user reconnects to the hacker's laptop, PDA, or other device. Now the hacker, with a different wireless interface, connects to the real wireless LAN, passing all authentication traffic to the real wireless network. The victim is oblivious to this and passes all data through the hacker. This scenario is possible because VPNs establish their connection at Layer 3 in the OSI model, while wireless exists below the VPN, at Layer 1 and Layer 2 (Security Problems and Solutions for Wireless LANs White Paper, 2004). Once connected, the hacker can use tools like DSNIFF, Ettercap, IKEcrack, or other Man-in-the-Middle tools to downgrade or rollback VPN security until traffic is in either in clear-text, or begins using an easily-broken weak encryption. This is a common problem in most VPN protocols, such as IPSEC, PPTP, SSH, SSL and L2TP.

Type 3: A third class of impersonation attack involves an attacker pretending to be an enterprise AP advertising an enterprise SSID. A typical wireless client machine scans for the best AP and associates with it. Once a client has associated with an attacker's AP, a number of attacks can

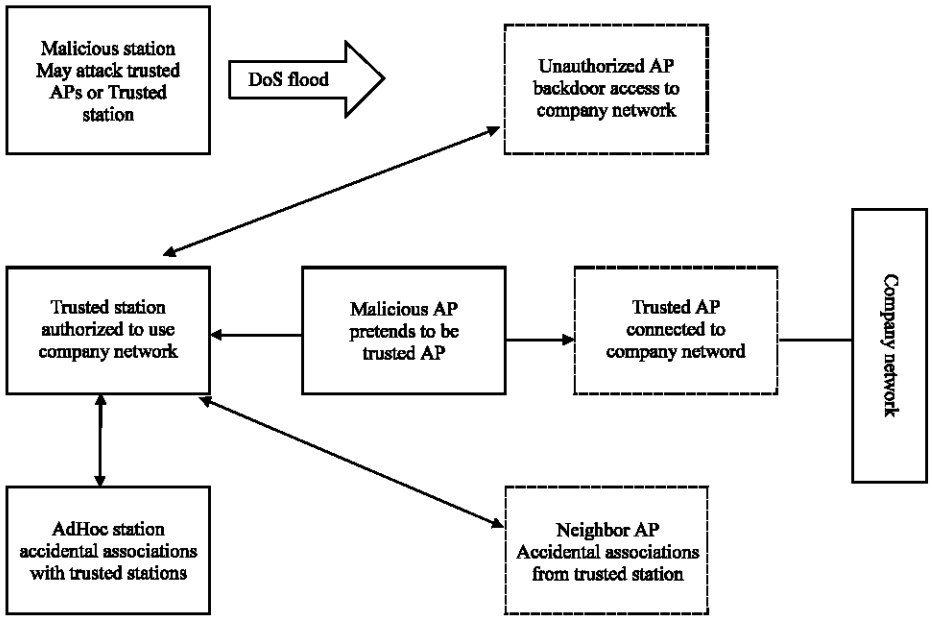

Fig. 1: Rogue devices and business risks

be carried out, including stealing authentication credentials, worm and virus transmission, or emulation of enterprise services for the purpose of stealing passwords.

Rouge APs and AdHoc networks: In an ideal world, the only wireless devices in or near one's facility would be known, trusted stations and Access Points (APs). But, as WLAN adoption grows, that becomes increasingly unlikely. Wireless transmissions from neighboring businesses and homes can easily bleed into one's facility, at distances ranging from yards to miles. Furthermore, contractors, customers, suppliers and other visitors to the facility are more likely than not to carry wireless-capable devices, including laptops, PDAs and tablet PCs. In this crowded environment, it can be tough to differentiate between friend and foe. Even the dividing line is not that simple. A new, previously-unknown AP may turn out to belong to a neighbor's network. It may be an unauthorized AP, installed by a well-intentioned but naive employee. Or it may be a malicious AP, hidden inside one's facility for the express purpose of gathering proprietary information. These and several other rogue examples are illustrated in Fig. 1.

In this study, the term Rogue is used to refer to all unauthorized wireless devices, operating within radio proximity, no matter what their intended purpose. Some common rouge APs are described next. Neighbor APs: 802.11 stations automatically associate with the best available AP, based on criteria like Extended Service Set Identifier (ESSID), received signal strength and data rates. As a result, trusted stations can accidentally associate with APs located upstairs, downstairs, next door, or down the street. AdHoc Associations: *AdHoc* associations may be used to conveniently share files or send documents to wireless-enabled printers. But peer-to-peer traffic completely bypasses network-enforced security measures like encryption and intrusion prevention. Unauthorized APs: Employees accustomed to wireless convenience at home or on the road often bring unauthorized APs into the office, connecting to the nearest Ethernet. Guests inside a building and war drivers outside the facility can use unauthorized APs to steal bandwidth, send objectionable content, retrieve confidential data, attack company assets, or use the network to attack others. Malicious APs: Malicious AP uses the same SSID as the trusted AP. Stations receiving stronger signal from the malicious AP associate with it instead of the trusted AP. The malicious AP can then record, add, delete, or modify frames exchanged between the station and trusted AP (Lisa, 2004).

RECOMMENDATION

After detailed analysis of the threats mentioned above and comparing existing solutions provided by various security organizations (e.g., AirDefense Inc. (2004) Aruba Wireless Networks Inc. (2004) AirMagnet Inc. (2004) etc.), the following are the observations and recommendations:

- In the earlier days of wireless LANs, an SSID operated like a shared password-only those who knew the SSID would be able to associate to the network. With the advent of wireless-aware operating systems such as Windows XP, this principle has become obsolete since long. However, some myths still persist. Some suggest disabling transmission of the network's SSID in beacon frames as a means to hide it. In reality, this practice does little to increase security. A war-driver running a passive network discovery tool may be discouraged by the missing SSID, but any active discovery tool, including Windows XP, will send out probe requests to learn the SSID. One can disable responses to broadcast probe requests, but this again only discourages the casual Internet-seeker. In reality, all it takes is a few minutes of sniffing the network or a few 2nd of running a Linux-based tool such as ESSID_Jack, to learn the SSID. Enabling the two previously discussed methods of hiding the SSID should be viewed as techniques to reduce probing by war-drivers rather than security techniques. So the threat, Probing/Network Discovery, can't be totally eradicated.
- There is a number of security features used to identify and prevent 802.11 DoS attacks. These include RF fingerprinting, signature detection, association flood detection, frame rate anomaly detection, rate limiting for 802.11 management frames and detection of MAC address spoofing. The net result is that many attacks are prevented, while all attacks are logged and reported to the network manager. These reports typically include the time, the type of attack, the target of the attack and the approximate physical location of the attack.
- As we can not lock the air, it is impossible to prevent wardrivers from eavesdropping. The key to preventing surveillance is the use of strong encryption-since it can not be controlled who receives the data, it should be made unreadable to unauthorized parties. Three types of data encryption are in wide use on wireless networks today, each with some variants: WEP, TKIP and IPSEC. But hackers may use tools like WEPwedgie, WEPCrack, WEPAttack, BSD-Airtools and AirSnort to break the encryption standards. These tools exploit vulnerabilities in the encryption algorithms by passively observing wireless LAN traffic until they collect enough data to recognize the pattern. They then use this information to break the encryption key. Care should, therefore, be taken in selecting the appropriate algorithm and IPSEC is suggested because, of all the known algorithms, IPSEC is the least vulnerable.
- There is a misconception that identity theft is only feasible if the MAC address is used for authentication and that 802.1×schemes such as LEAP are totally safe. Cracking LEAP to steal identity has become easy with tools like ASLEAP and THC-LeapCracker. Other authentication schemes, such as EAP-TLS and PEAP, may require more sophisticated attacks that exploit other known vulnerabilities in wired side authentication schemes, but are feasible. RF monitoring allows users to ensure that proper authentication is being enforced. In addition, excessive authentication attempts may also indicate a malicious attempt by a hacker.
- Only a highly capable Intrusion Detection System (IDS) and 24 h monitoring can detect Type 2 Impersonation attacks on a wireless LAN. An effective security solution keeps a constant watch on the network, while simultaneously analyzing the network activity. Since this type of attack is not based on a single signature, a wireless IDS must be able to correlate and analyze data to show that this type of attack is occurring.
- Protecting against honeypot attack (Type 3 Impersonation) includes monitoring usage of the enterprise SSID and disabling any unauthorized APs using it.
- The obvious way to find unauthorized networks is to do the same thing that attackers do: use an antenna and look for them so that unauthorized networks could be found before attackers exploit them. Physical site audits should be conducted as frequently as possible. The trade-off is that more frequent audits are more likely to catch unauthorized deployments, but the high cost of staff time may make walk-through detection untenable in all but the most sensitive environments. One potential compromise is to select a tool based on a small handheld form factor such as the Compaq iPAQ and have help desk technicians use handheld scanners to detect unauthorized networks while responding to user support calls throughout the campus.

CONCLUSION

As businesses and consumers continue their rapid adoption of wireless technologies, all enterprises must address the growing security concerns from new airborne threats. When a company network is left exposed by

insecure devices, hackers can enter the organization and compromise corporate backbone of the company, rendering investments in information technology security obsolete. The implications from a security breach can impact the company's reputation, intellectual property and regulated information. Building secure IT infrastructure from the start can be less expensive than adding it later. Preventing security breaches is less expensive than the cost of recovery and downtime. Start by understanding the threats and vulnerabilities outlined in this paper, assess business impact and apply appropriate security strategies to safely take advantage of mobile and wireless for improved productivity and competitive advantage.

REFERENCES

Mitchell Ashley, 2004. A Guide To Wireless Network Security. Technical White Paper, Latis Networks Inc.

Wireless LAN Security, 2004. What Hackers Know That You Don't. Technical White Paper, AirDefense Inc.

Joris Claessens Bart Preneel and Joos Vandewalle, 2002. Combining World Wide Web and Wireless Security. Informatica, 26: 123-132.

Secure Wireless-What Vendors Don't Tell You, 2004. A Technical Discussion on Wireless Attacks and the Use of Multi-Layered Wireless Security. Technical White Paper, Aruba Wireless Networks Inc.

Claire McDonough, 2003. Identifying The Risks Involved in Allowing Wireless Portable Devices Into Your Company. Version 1.4b, Option 1, SANS Institute.

Robert, J. Shimonski, 2004. Wireless Attacks Primer. Internet Software Marketing Ltd.

Robert, J. Shimonski, 2004. Wireless Security Primer 101. Internet Software Marketing Ltd.

Robert, J. Shimonski, 2004. Wireless Security Primer (Part II). Internet Software Marketing Ltd.

Dung Chang, 2002. Security Along the Path Through GPRS Towards 3G Mobile Telephone Network Data Services. Version 1.3, SANS Institute.

Security Problems and Solutions for Wireless LANs White Paper, 2004. Technical White Paper, ActivCard Corporation.

Lisa Phifer, 2004. Best Practices for Rogue Detection and Anhilation. Technical White Paper, AirMagnet Inc.